



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50



Edição nº 1.959
27 de maio de 2024

PORTARIA Nº 1.513/2024
DE 27 DE MAIO DE 2024

Institui o Plano Diretor de Proteção de Dados Pessoais do Ministério Público do Estado de Sergipe (MPSE), e dá outras providências.

O **PROCURADOR-GERAL DE JUSTIÇA**, no uso de suas atribuições legais conferidas pela Lei Federal nº 8.625, de 12 de fevereiro de 1993, e pela Lei Complementar Estadual nº 02, de 12 de novembro de 1990, e

Considerando que a proteção de dados pessoais é direito fundamental autônomo na Constituição Federal de 1988 (art. 5º, inciso LXXIX);

Considerando que o princípio da segurança, previsto no art. 6º, inciso VII, da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados), obriga a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

Considerando que o princípio da prevenção, consagrado no art. 6º, inciso VIII, da Lei nº 13.709/2018, impõe a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Considerando que o princípio da *accountability* (responsabilização e prestação de contas) exige a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas, conforme se extrai do art. 6º, inciso X, da Lei Geral



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

de Proteção de Dados;

Considerando que, de acordo com o art. 46 da Lei nº 13.709/2018, o Ministério Público do Estado de Sergipe, enquanto agente de tratamento de dados, deve “adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”;

Considerando que “a violação ou o vazamento de dados pessoais, voluntária ou acidentalmente, é considerado um incidente de segurança no tratamento, notadamente se ocasionar destruição, perda, alteração, subtração, cópia, transferência, comunicação ou difusão de dado pessoal”, nos termos do art. 135 da Resolução nº 281, de 12 de dezembro de 2023, do Conselho Nacional do Ministério Público (CNMP);

Considerando que “todo responsável pelo tratamento de dados pessoais deverá reportar ao Encarregado e ao órgão de tecnologia da informação competente, imediatamente, a ocorrência de incidente de segurança com dados pessoais, com finalidade de permitir a imediata tomada de medidas de contenção e outras necessárias ao controle e à mitigação do dano”, por força do disposto no art. 145 da Resolução nº 281/2023, do Conselho Nacional do Ministério Público;

Considerando que o Ministério Público de Sergipe, na qualidade de controlador, deverá adotar, para além de medidas técnicas, expedientes de ordem administrativas, como a criação de novas rotinas de trabalho, procedimentos de segurança de informação e aumento da transparência e governança, o que exigirá a criação e difusão de uma cultura de proteção de dados dentro da Instituição;

RESOLVE:

Art. 1º Institui o Plano Diretor de Proteção de Dados Pessoais do Ministério Público do Estado de Sergipe (MPSE), na forma do Anexo Único desta Portaria.



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

Art. 2º Os casos omissos desta Portaria serão submetidos a apreciação do Procurador-Geral de Justiça para deliberação.

Art. 3º Esta Portaria entra em vigor na data de sua publicação no Diário Oficial Eletrônico do Ministério Público do Estado de Sergipe (DOFe MPSE).

Art. 4º Ficam revogadas as disposições em contrário.

Dê-se ciência, cumpra-se e publique-se.

Manoel Cabral Machado Neto
Procurador-Geral de Justiça



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

PORTARIA Nº 1.513/2024
DE 27 DE MAIO DE 2024

ANEXO ÚNICO

PLANO DIRETOR DE PROTEÇÃO DE DADOS PESSOAIS
Lei Geral de Proteção de Dados Pessoais (LGPD)

1. INTRODUÇÃO

Este documento materializa o Plano Diretor de Proteção de Dados Pessoais do Ministério Público do Estado de Sergipe (MPSE), em consonância com as disposições da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), e da Resolução nº 281, de 12 de dezembro de 2023, do Conselho Nacional do Ministério Público (CNMP), que instituiu a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público. Este plano visa a estabelecer estrutura e diretrizes claras para garantia da proteção efetiva dos dados pessoais sob a responsabilidade desta Instituição.

A legislação determina que a gestão pública vincule o tratamento de dados pessoais ao cumprimento de sua finalidade pública, visando ao interesse público, para executar as competências legais ou cumprir as atribuições legais afetas ao serviço público.

A Resolução CNMP nº 281/2023, no art. 35, estipula a criação do Plano Diretor de Proteção de Dados Pessoais, o qual deve abranger o funcionamento, os procedimentos (incluindo reclamações e petições dos titulares), as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e mitigação de riscos, e outros aspectos relacionados ao tratamento de dados pessoais.

Com base no compromisso com a transparência e a segurança dos dados dos cidadãos, este documento tem como objetivo principal fornecer um roteiro abrangente de atividades necessárias para garantir a conformidade com as exigências legais e promover uma cultura de proteção de dados dentro do Ministério Público do Estado de Sergipe.

O método utilizado prioriza a execução de ações de melhoria contínua, com vistas ao cumprimento das diretrizes fixadas pela LGPD. Para isso, desenvolvem-se estratégias e ações específicas, alinhadas com as melhores práticas adotadas nos órgãos públicos do país, cuja implementação garantirá a proteção adequada dos dados pessoais e o cumprimento da legislação em vigor.



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

Ressalta-se que este plano se fundamenta em boas práticas, levando em consideração a estrutura organizacional do Ministério Público do Estado de Sergipe, assegurando que as atividades propostas sejam adequadas à realidade e às necessidades específicas desta Instituição. Eventuais lacunas identificadas no decorrer da implementação serão devidamente corrigidas durante a própria execução do plano, de forma a propiciar abordagem abrangente e eficaz na proteção dos dados pessoais.

2. DEFINIÇÕES GERAIS

Para os efeitos deste Plano Diretor, considera-se:

- I – Dado Pessoal: informação relativa à pessoa natural identificada ou identificável;
- II – Dado Pessoal Sensível: dado de pessoa natural referente à sua origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, à saúde, à vida sexual, à genética ou biométrica;
- III – Dado Anonimizado: dado relativo a titular que não possa ser identificado, a partir da utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- IV – Banco de Dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
- V – Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- VI – Controlador: responsável pelas decisões relativas ao tratamento de dados pessoais, que, no âmbito do Ministério Público do Estado de Sergipe, competem à Procuradoria-Geral de Justiça;
- VII – Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador;
- VIII – Encarregado: pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- IX – Agentes de Tratamento: o Controlador e o Operador;
- X – Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
- XI – Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- XII – Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

XIII – Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XIV – Atividade-meio: revestida de caráter administrativo e voltada à organização e ao funcionamento do Ministério Público do Estado de Sergipe, no âmbito de sua autonomia administrativa, financeira e orçamentária, conforme o disposto, entre outros, no art. 127, § 2º, da Constituição Federal;

XV – Atividade-fim: regida pelos princípios institucionais da unidade, da indivisibilidade e da independência funcional e voltada ao desempenho das atribuições constitucionais e legais do Ministério Público do Estado de Sergipe, conforme o estabelecido, entre outros, pelos arts. 127, caput e § 1º, e 129 da Constituição Federal.

XVI – Autoridade Nacional de Proteção de Dados: os arts. 55-A e seguintes da Lei Geral de Proteção de Dados (LGPD) definem a Autoridade Nacional de Proteção de Dados (ANPD), entidade responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional;

XVII – Incidente: evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XVIII – Incidente de Segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XIX – Incidente de Segurança com Dados Pessoais: de acordo com a Autoridade Nacional de Proteção de Dados (ANPD), incidente de segurança à proteção de dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares dos dados pessoais;

XX – Relatório Final: Relatório contenha todas as evidências e ações realizadas para tratamento do incidente e que deve ser emitido ao final das tratativas;

XXI – Relatório de Impacto a Proteção de Dados (RIPD): conforme a LGPD, o Relatório de Impacto a Proteção de Dados (RIPD) é uma documentação do Controlador que contém a descrição dos processos de tratamento de dados pessoais que tem o potencial de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco;



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

XXII – Sistema de Inteligência Artificial (sistema de IA): programa informático desenvolvido capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage; e

XXIII – Ferramentas de Inteligência Artificial Generativa: sistemas ou algoritmos que utilizam técnicas de aprendizado de máquina para criar e gerar novos dados, geralmente na forma de texto, imagens, áudio ou vídeos.

3. ESTRUTURA ADMINISTRATIVA DE PROTEÇÃO DE DADOS PESSOAIS

3.1. Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP)

O Ministério Público do Estado de Sergipe, por meio da Portaria nº 916/2024, datada de 04 de abril de 2024, instituiu o Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP), órgão vinculado à Procuradoria-Geral de Justiça.

Conforme estabelecido pelo art. 2º da acima referenciada Portaria, o CEPDAP é composto por:

- I – Encarregado de Proteção de Dados;
- II – 1 (um) membro indicado pela Corregedoria-Geral do MPSE;
- III – 1 (um) membro ou servidor indicado pela Ouvidoria do MPSE;
- IV – Secretário-Geral da Procuradoria-Geral de Justiça;
- V – Diretor do Gabinete de Segurança Institucional; e
- VI – Diretor de Tecnologia da Informação e Comunicação.

3.1.1. Competências do CEPDAP

O Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) possui, nos termos do art. 3º da Portaria 916/2024, as seguintes atribuições:

- I – orientar o Controlador e o Encarregado nas questões afetas à proteção ou governança de dados pessoais;
- II – propor as prioridades dos investimentos em proteção de dados pessoais, para análise e decisão da Chefia da Instituição;
- III – coordenar o processo de elaboração e revisão do Plano Diretor de Proteção de Dados Pessoais;
- IV – monitorar a execução do Plano Diretor de Proteção de Dados Pessoais e adotar as providências necessárias à sua implementação e ao seu cumprimento;
- V – produzir diagnósticos, estudos e avaliações periódicas a respeito do Plano Diretor de Proteção de Dados Pessoais;
- VI – opinar sobre a elaboração, revisão, aprovação e publicação de Relatórios de Impacto à Proteção de Dados Pessoais;



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

VII – propor mecanismos e instrumentos para a investigação e a prevenção de quebra de segurança da informação relativa a dados pessoais, bem como para o tratamento da informação sigilosa comprometida concernente a dados pessoais;

VIII – sugerir critérios acerca da publicidade dos atos quando envolverem a exibição de dados pessoais mantidos pelo Ministério Público;

IX – opinar sobre outras questões afetas à proteção de dados pessoais, inclusive sobre o tratamento dos dados pessoais decorrente do uso de inteligência artificial pelo Ministério Público; e

X – promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgãos.

3.2. Encarregado pelo Tratamento de Dados Pessoais

Nos termos do art. 44 da Resolução CNMP nº 281/2023, o Encarregado é a pessoa indicada pelo Controlador para atuar como canal de comunicação e interação entre o Controlador, os titulares dos dados pessoais e a Autoridade de Proteção de Dados Pessoais do Ministério Público (APDP/MP). Além disso, o Encarregado é responsável por desempenhar outras funções estabelecidas tanto pela legislação quanto pela própria Resolução citada.

O Encarregado pelo Tratamento de Dados Pessoais, no âmbito do Ministério Público do Estado de Sergipe, será um Promotor de Justiça com experiência e conhecimentos sobre proteção de dados pessoais.

A identidade e as informações de contato do Encarregado encontram-se disponíveis no Portal LGPD, localizado no sítio eletrônico do MPSE, de maneira acessível e de fácil compreensão, promovendo a transparência e a conformidade com as normativas vigentes acerca do tema.

3.2.1. Competências do Encarregado:

Compete ao Encarregado pelo Tratamento de Dados Pessoais do Ministério Público do Estado de Sergipe, nos termos do art. 46 da Resolução nº 281/2023, do Conselho Nacional do Ministério Público:

I – implementar, capacitar, conscientizar, estabelecer responsabilidades e monitorar a conformidade da atuação da Instituição com a Política Nacional de Proteção de Dados Pessoais no Ministério Público e a LGPD;

II – receber e analisar os pedidos encaminhados pelos titulares dos dados pessoais, como reclamações e comunicações, prestar esclarecimentos e adotar providências relacionadas ao tratamento de dados pessoais;

III – delegar, inclusive para servidores, e supervisionar atribuições que não representem risco relevante ao titular de dados pessoais;

IV – elaborar e manter inventário de dados pessoais que documente como e por que o Ministério Público coleta, compartilha e usa esses dados;



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

V – recomendar e orientar a confecção dos Relatórios de Impacto à Proteção de Dados Pessoais (RIDP) e monitorar a sua correta realização;

VI – informar e emitir recomendação ao Controlador e ao Operador;

VII – cooperar, interagir e consultar com a APDP/MP; e

VIII – executar as demais atribuições determinadas pelo Controlador ou estabelecidas em normas complementares.

Para além das atribuições previstas na Resolução CNMP nº 281, compete ao Encarregado, segundo o art. 7º da Portaria nº 2.136/2022:

I – coordenar a elaboração, a implantação e o monitoramento da política de privacidade e proteção de dados pessoais do MPSE;

II – implementar e monitorar a conformidade da atuação da Instituição com o Programa de Proteção de Dados Pessoais e a LGPD;

III – informar e emitir recomendação de adequação ao Controlador ou aos Operadores de tratamento de dados;

IV – aconselhar os órgãos do MPSE sobre questões relacionadas ao Relatório de Impacto a Proteção de Dados (RIPD) bem como monitorar sua performance;

V – receber comunicações, cooperar com a Autoridade Nacional de Proteção de Dados (ANPD) e adotar providências;

VI – atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;

VII – receber e analisar os pedidos encaminhados pelos titulares dos dados, podendo requisitar ou solicitar aos Controladores/Operadores dos dados as informações necessárias para tal finalidade;

VIII – viabilizar o acesso dos titulares aos dados que lhes digam respeito;

IX – determinar aos órgãos do MPSE a adoção de providências para a correção de dados pessoais incompletos, inexatos ou desatualizados;

X – responder solicitação, interna ou externa, relacionada ao tratamento de dados pessoais;

XI – atuar com base no risco associado às operações de tratamento realizadas pela Instituição, levando em consideração a natureza, o escopo, o contexto e o propósito do tratamento;

XII – orientar os membros, servidores e contratados da Instituição a respeito das práticas a serem tomadas em relação à proteção de dados pessoais e promover sua capacitação e sensibilização sobre os cuidados necessários com o tratamento dos dados pessoais;

XIII – auxiliar o Controlador a responder a incidentes de segurança e vazamentos de dados;



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

XIV – assessorar o Controlador a comunicar à Autoridade Nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares;

XV – adotar providências relativas às comunicações recebidas da Autoridade Nacional, dando ciência ao Procurador-Geral de Justiça;

XVI – elaborar e manter, em conjunto com as unidades da Instituição, inventário que documente como e por que o MPSE coleta, compartilha e usa dados pessoais;

XVII – assegurar a incorporação da privacidade, bem como do programa de proteção de dados pessoais e diretrizes estabelecidas na LGPD, desde a concepção de mecanismos que venham a ser implementados na Instituição, a fim de garantir a efetividade dos direitos dos titulares de dados;

XVIII – sugerir ao órgão de segurança da informação medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

XIX – formular princípios e diretrizes para a gestão de dados pessoais e propor orientações sobre o tratamento dos dados pessoais, de acordo com as diretrizes estabelecidas na LGPD e nas normas internas;

XX – propor a formulação de regras de boas práticas e de governança que estabeleçam as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas e os mecanismos internos de supervisão e de mitigação de riscos;

XXI – promover as ações necessárias à adequação dos documentos elaborados pelos órgãos da administração, de execução e auxiliares da Instituição, podendo, para tanto, recomendar sua adequação;

XXII – garantir a necessária observância dos órgãos administrativos responsáveis pelos contratos e convênios firmados pela Instituição às diretrizes da LGPD, mediante a inserção de cláusulas expressas de observância à lei;

XXIII – auxiliar o Controlador a fazer o inventário e o mapeamento dos dados pessoais que trafegam na Instituição, identificando os processos de trabalho nos quais são coletados e os documentos em que são inseridos;

XXIV – promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgãos;

XXV – assessorar o Procurador-Geral de Justiça em questões e matérias relacionadas à proteção de dados pessoais, em especial no que toca à interpretação e à aplicação da legislação vigente sobre o tema; e



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

XXVI – exercer outras atividades correlatas com as competências anteriormente estabelecidas, ainda que não expressamente elencadas, outras atividades criadas pelo Controlador e/ou estabelecidas, por meio de normas complementares, pela Autoridade Nacional.

4. TRATAMENTO DE DADOS PESSOAIS

O Ministério Público do Estado de Sergipe instituiu, por meio da Portaria nº 2.136/2022, a Política de Privacidade e de Proteção de Dados Pessoais, a qual prevê que, no exercício da atividade-meio e da atividade-fim, o MPSE coletará dados pessoais (inclusive sensíveis e de crianças e adolescentes) apenas na extensão necessária ao desempenho de suas funções, com a observância do regime de tratamento aplicável em cada caso, conforme a legislação vigente e de acordo com as disposições do referido Ato.

Ainda, a Portaria dispõe que os dados pessoais poderão ser coletados, no Portal do Ministério Público do Estado de Sergipe na Internet, através de representações, cadastros de manifestações, formulários de atendimento, *cookies*, entre outros meios necessários para o cumprimento de suas funções, bem como deixa claro que poderá haver coleta de dados pessoais através da interoperabilidade de sistemas, bem como dos atendimentos realizados pela Corregedoria-Geral, pela Ouvidoria do Ministério Público, pelo Setor de Triagem, e pelas Promotorias e Procuradorias de Justiça, presencial ou virtualmente, dos sistemas de controle e de acesso às instalações da instituição, atividades preventivas imprescindíveis à salvaguarda da Instituição, correio eletrônico, intranet, sistemas de troca de mensagens, preenchimento de cadastros para fins funcionais, contratuais e licitatórios.

De acordo ainda com a Política de Privacidade e de Proteção de Dados Pessoais (Portaria nº 2.136/2022), o Ministério Público do Estado de Sergipe, nas suas atividades finalísticas, poderá realizar o tratamento de dados pessoais, inclusive sensíveis e de crianças e de adolescentes, independentemente do consentimento dos titulares, sempre que necessário ao cumprimento de suas atribuições e prerrogativas constitucionais, sendo que o tratamento de dados pessoais será limitado ao mínimo necessário para a realização de sua finalidade.

Segundo a Portaria nº 2.136/2022, o Ministério Público do Estado de Sergipe, no exercício de suas atividades administrativas não vinculadas diretamente ao exercício de suas competências legais e constitucionais, somente poderá realizar o tratamento de dados pessoais nas seguintes hipóteses:

- I – para o cumprimento de obrigação legal ou regulatória;
- II – para a realização de estudos por órgão de pesquisa, via anonimização dos dados pessoais, sempre que possível;
- III – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido deste;
- IV – para o exercício regular de direitos em processo judicial ou administrativo;



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

- V – para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- VI – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- VII – quando necessário para atender aos interesses legítimos do Controlador ou de terceiro, exceto no caso de tratar-se de dados pessoais sensíveis ou de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; e
- VIII – mediante o fornecimento de consentimento pelo titular.

Qualquer pessoa interessada em acessar sistemas e serviços existentes nos portais e canais de comunicação oficiais do órgão deverá fornecer seus dados pessoais na extensão que, em cada caso, for necessária à garantia da qualidade, integridade e segurança das informações que lhe forem prestadas.

Com vistas ao regular exercício do consentimento, o MPSE manterá Aviso de Privacidade nos portais e canais de comunicação oficiais, com informações a respeito de suas atribuições institucionais e da necessidade de coleta e uso dos dados pessoais do titular interessado em acessar sistemas e serviços da Instituição.

4.1. Exceções que autorizam o tratamento de dados pessoais

O art. 72 da Resolução CNMP nº 281/2023 prevê ser legítimo o tratamento de dados pessoais nas atividades imprescindíveis à segurança da sociedade ou institucional, sobretudo para o não comprometimento das atividades de produção de conhecimento, bem como de investigação ou fiscalização, relacionadas com a prevenção ou repressão de infrações.

Dessa forma, para o exercício de suas atribuições, não se aplica ao Ministério Público a restrição de acesso a dados pessoais, quando as informações colhidas se destinarem a atividades de segurança pública, de produção de conhecimento ou de atividades de investigação e repressão de infrações penais, para o exercício da segurança institucional, bem como quando forem destinadas à sua atividade finalística, compreendida nela todas as atribuições legais contidas na Constituição Federal, notadamente as ações e atribuições inseridas no art. 129 da Carta Magna, além da legislação infraconstitucional que lhe confere concretude.

Dispõe ainda que o Ministério Público, ao utilizar técnicas de vigilância, monitoramento e controle, no desenvolvimento das suas atividades preventivas e persecutórias em prol da defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis, bem como da produção de conhecimento imprescindível à concretização dessas obrigações constitucionais e, ainda, da salvaguarda dos ativos da Instituição, deverá adotar medidas de cautela para reforço da proteção dos dados pessoais, incluindo, dados pessoais referentes a DNA, voz, imagem facial, reconhecimento automatizado (inclusive facial), expressão corporal (inclusive trejeitos e modo de andar), impressões digitais e outros dados biométricos ou de comportamento.



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, garantido o devido processo legal com contraditório e ampla defesa, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

4.2. Dados pessoais sensíveis

No tratamento de dados pessoais sensíveis, para instruir investigação de natureza cível ou criminal, para as ações de segurança institucional, de produção de conhecimento, no âmbito de seus procedimentos extrajudiciais ou na atuação em processos judiciais, bem como nos bancos de dados pessoais mantidos para conferir suporte a tais atividades, o MPSE agirá com reforço de proteção e cuidados específicos nas suas etapas.

Segundo o art. 84 da Resolução CNMP nº 281/2023, o tratamento de dados pessoais sensíveis, nas atividades administrativas do órgão, deverá ser realizado mediante consentimento expreso e específico do titular ou de seu representante legal, podendo ser dispensado, entre outros, nos seguintes casos:

- I – cumprimento de obrigação legal ou regulatória pelo Controlador;
- II – tratamento compartilhado de dados necessários à execução, pelo Ministério Público, de políticas públicas previstas em leis ou regulamentos;
- III – tratamento necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular;
- IV – exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- V – tratamento necessário à declaração, ao exercício ou à defesa de direitos em procedimento extrajudicial ou processo administrativo;
- VI – tratamento necessário por motivos de interesse público, que deve ser proporcional em relação ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular;
- VII – proteção da vida ou da incolumidade física do titular ou de terceiro;
- VIII – proteção de interesses vitais do titular dos dados pessoais ou de terceiro, se o titular estiver física ou legalmente impossibilitado de dar o seu consentimento;
- IX – garantia de prevenção à fraude e de segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
- X – tratamento relacionado com dados pessoais manifestamente tornados públicos pelo seu titular;



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

XI – tratamento efetuado por fundações, associações ou outros organismos sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais;

XII – tratamento necessário por motivos de interesse público no domínio da segurança pública e institucional;

XIII – tratamento necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica, ou para fins estatísticos, devendo ser proporcional em relação ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguem os direitos fundamentais e os interesses do titular; e

XIV – tratamento necessário às atividades de segurança institucional e de produção de conhecimento para o exercício das funções finalísticas do Ministério Público.

Dar-se-á publicidade à dispensa de consentimento nos casos de aplicação do disposto nos itens I e II, pelos órgãos competentes do MPSE, nos termos do inciso I do *caput* do art. 23 da LGPD.

4.3. Dados pessoais de crianças e de adolescentes

Os dados pessoais de crianças e de adolescentes serão tratados visando ao seu melhor interesse, conforme a legislação vigente, sobretudo as disposições da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente).

O tratamento de dados pessoais de crianças será realizado, em regra, com o consentimento de, pelo menos, um dos pais ou do responsável legal, podendo ser coletados sem o consentimento, quando a coleta for necessária para contatar os pais, ou o responsável legal, ou para sua proteção.

O Controlador e o responsável pelo tratamento devem realizar todos os esforços razoáveis para verificar se o consentimento, quando necessário, foi dado pelo responsável pela criança ou pelo adolescente.

Nos termos do art. 88 da Resolução CNMP nº 281/2023, no tratamento de dados pessoais de crianças e adolescentes desempenhado no âmbito da atividade administrativa do Ministério Público, o Controlador, ressalvadas as hipóteses previstas no § 2º do art. 66 da referida Resolução, deverá manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 da LGPD.

As informações a respeito do tratamento de dados de crianças ou adolescentes deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físicas, perceptivas, sensoriais, mentais e intelectuais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança ou adolescente.



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

O tratamento de dados pessoais de crianças e adolescentes, iniciado em data anterior à vigência da LGPD e ainda não finalizado, deverá, quando necessário e possível, ser informado a pelo menos um dos pais ou responsável legal e colhido o consentimento para a continuidade da operação.

Na coleta de dados pessoais de crianças e adolescentes, todos os registros deverão, quando possível, estar acompanhados de documento válido que comprove essa peculiar condição pessoal.

4.4. Término do tratamento de dados pessoais

O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I – verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II – fim do período de tratamento;

III – comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público;

IV – determinação da autoridade nacional, quando houver violação ao disposto na legislação vigente que trata da proteção de dados pessoais.

Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I – cumprimento de obrigação legal ou regulatória pelo Controlador;

II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta norma; ou

IV – uso exclusivo do Controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

5. COMPARTILHAMENTO DE DADOS PESSOAIS

O MPSE, observadas as disposições da Lei Geral de Proteção de Dados Pessoais, da Resolução nº 281/2023, do CNMP e da Portaria nº 2.136/2022, poderá realizar o compartilhamento de dados pessoais tratados na sua atividade-meio ou atividade-fim, para a execução de suas atribuições legais, realização de políticas públicas e cumprimento de obrigações legais ou regulatórias.

A Instituição apenas transferirá os dados pessoais existentes em suas bases de dados para entidades privadas nas seguintes hipóteses:



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

I – necessidade relativa à execução descentralizada de atividade institucional que exija a transferência, tão somente na extensão indispensável ao alcance desse fim específico e determinado;

II – os dados compartilhados já são acessíveis publicamente;

III – existência de previsão da transferência em atos normativos, contratos, convênios ou instrumentos congêneres;

IV – prevenção de fraudes e irregularidades, proteção ou resguardo da segurança e integridade do titular dos dados pessoais.

Conforme previsto no art. 94, § 1º, da Resolução CNMP nº 281/2023, o compartilhamento seguro de bases de dados pessoais entre o CNMP, os ramos e as unidades do Ministério Público, bem como a transferência segura de dados pessoais, deverão ser formalizados, cabendo aos órgãos envolvidos informar a origem da base de dados e atestar o seu recebimento e a sua integridade, ficando dispensada a celebração de convênio, acordo de cooperação técnica ou instrumento congênere para a efetivação do compartilhamento de dados pessoais previstos no dispositivo.

Finalizada a transferência e o compartilhamento seguro, o órgão ministerial que os concretizou não será responsabilizado pelos incidentes de segurança por ventura ocasionados pelo tratamento realizado pelo órgão ou pela instituição que os recebeu.

Respeitados o sigilo empresarial e as demais proteções legais, o MPSE pode requisitar, a qualquer tempo, informações a respeito do tratamento dos dados pessoais confiados a fornecedores de produtos, prestadores de serviços ou parceiros, que, ao tratarem os dados pessoais a eles confiados pela Instituição, são considerados Operadores e sujeitam-se às disposições da Portaria nº 2.136/2022, de modo que, para além dos respectivos deveres legais e contratuais, devem observar as seguintes obrigações:

I – assinar contrato ou termo de compromisso com cláusulas específicas sobre proteção de dados pessoais definidas pelo Ministério Público do Estado de Sergipe;

II – apresentar evidências e garantias suficientes de que aplica medidas técnicas e administrativas adequadas de segurança para a proteção dos dados pessoais, nos termos definidos na legislação, em atos normativos do Ministério Público do Estado de Sergipe e nos instrumentos contratuais;

III – manter os registros de tratamento de dados pessoais que realiza em condições de rastreabilidade e de fornecimento de prova eletrônica a qualquer tempo;

IV – seguir as diretrizes e instruções transmitidas pelo Ministério Público do Estado de Sergipe;

V – facultar acesso a dados pessoais apenas em casos estritamente necessários, para pessoa autorizada que tenha assumido compromisso formal de preservar a confidencialidade e segurança de tais dados, devendo a prova do compromisso estar disponível em caráter permanente para exibição ao Ministério Público do Estado de Sergipe, em caso de solicitação;



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

VI – permitir a realização de auditorias, incluindo inspeções pelo Ministério Público do Estado de Sergipe ou por quem por ele autorizado, e disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações estabelecidas;

VII – auxiliar, sempre que demandado pelo Ministério Público do Estado de Sergipe, no atendimento de obrigações perante os titulares de dados pessoais, autoridades competentes ou quaisquer outros legítimos interessados;

VIII – comunicar, de maneira formal e imediata ao Encarregado pelo Tratamento de Dados Pessoais do MPSE, a ocorrência de qualquer risco, ameaça ou incidente de segurança que possa comprometer ou causar dano potencial ou efetivo a titular de dados pessoais, evitando atrasos por conta de verificações ou inspeções;

IX – anonimizar ou devolver todos os dados pessoais existentes e descartar, de forma irrecuperável, as cópias, após a satisfação da finalidade respectiva ou o encerramento do tratamento por decurso de prazo ou por extinção de vínculo legal ou contratual.

6. SEGURANÇA E DAS BOAS PRÁTICAS

Por meio da Portaria nº 2.136/2022, foi instituída a Política de Privacidade e de Proteção de Dados Pessoais do MPSE, que prevê a contínua implementação de medidas físicas, técnicas e administrativas necessárias à garantia e ao incremento da segurança da informação, visando a proteger os dados tratados e seus titulares de acessos não autorizados e de qualquer outro incidente que evidencie tratamento inadequado.

A Portaria estabelece, em seu artigo 18, que é dever dos membros, servidores e colaboradores do Ministério Público do Estado de Sergipe cumprir integralmente os termos da Política de Privacidade no desempenho de suas atividades.

Eventual descumprimento deverá ser comunicado imediatamente ao Encarregado, o que também poderá ser realizado pelo titular cujo direito à proteção de dados pessoais houver sido objeto de alguma violação. Ainda, a inobservância do disposto na normativa em questão poderá implicar responsabilização nas esferas criminal, civil e administrativa.

O Encarregado ao ser comunicado de violação da LGPD, da Resolução CNMP nº 281 ou de demais atos normativos internos referentes à proteção de dados pessoais, comunicará o fato ao Procurador-Geral de Justiça para a adoção das providências pertinentes.

Além disso, para proteção de dados pessoais contra acessos não autorizados, situações acidentais e incidentes culposos ou dolosos de perda, destruição, adulteração, compartilhamento indevido ou outro tipo de tratamento inadequado ou ilícito, serão observadas as medidas técnicas e administrativas previstas na Política de Segurança Institucional do Ministério Público do Estado de Sergipe, bem como nos atos normativos e técnicos específicos sobre segurança da informação.

Com o intuito de disseminar a cultura sobre as boas práticas a serem adotadas em relação à proteção de dados pessoais, a Instituição busca promover ações e programas para capacitação e conscientização de seus membros, servidores e colaboradores.



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

7. PROGRAMA DE GOVERNANÇA EM PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

A governança de dados refere-se aos processos e políticas que uma organização adota para garantir a integridade, segurança e a conformidade legal de seus dados.

Tanto o art. 50 da LGPD quanto os arts. 35 e 111 da Resolução CNMP nº 281/2023 dispõem sobre a elaboração de Programa de Governança em Privacidade e Proteção de Dados Pessoais, que deve incluir, no mínimo, os seguintes elementos constitutivos:

- I – estruturação, organização e regime de funcionamento;
- II – canal de comunicação para titular de dado pessoal;
- III – definição de normas de segurança;
- IV – definição das responsabilidades aos agentes de tratamento de dados;
- V – implantação de ações educativas e de capacitação;
- VI – estabelecimento dos mecanismos de gestão e mitigação de riscos;
- VII – identificação da natureza do dado pessoal;
- VIII – comprometimento do Controlador com proteção de dados;
- IX – aplicação do programa a todo o conjunto de dados pessoais;
- X – adaptação à estrutura, à escala e ao volume das operações do órgão;
- XI – definição de medidas para avaliação de impactos e riscos à privacidade;
- XII – criação de relação de confiança entre instituição e titular de dados;
- XIII – integração a sua estrutura geral de governança, estabelecimento e aplicação de mecanismos de supervisão internos e externo;
- XIV – previsão de planos de resposta a incidentes e remediação; e
- XV – atualização constante das boas práticas de governança.

O processo de implantação do Programa de Governança em Privacidade e Proteção de Dados Pessoais, conforme explicita a LGPD, pode ser dividido em três etapas:

- a) Planejamento e Iniciação: art. 50, § 2º, inciso I, alíneas “a” e “b”, da LGPD;
- b) Construção e Execução: art. 50, § 2º, inciso I, alíneas “c”, “d”, “e”, “f” e “g”, da LGPD;
- c) Monitoramento e Avaliação: art. 50, § 2º, inciso I, alínea “h”, da LGPD.

1ª Etapa: Planejamento e Iniciação

Nomeação do Encarregado de proteção de dados

Alinhamento de expectativas com a Administração Superior



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

Medidas de segurança do dado pessoal

Estrutura organizacional para governança e proteção de dados

Inventário de dados pessoais: mapeamento dos processos

Levantamento de contratos relacionados a dados pessoais

Diagnóstico e rastreabilidade de dados

2ª Etapa: Construção e Execução

Práticas para privacidade e proteção de dados pessoais.

Cultura de segurança de dados e privacidade desde a concepção.

Política de Privacidade e Proteção de Dados Pessoais: responsáveis, dados coletados e formas, cookies, tratamento, compartilhamento e transferência, medidas técnicas.

Adequação de cláusulas contratuais: resultados de inventário de contratos que impliquem tratamento de dados pessoais e ajustes.

Termos de Uso: regras sobre coleta, uso, tratamento e proteção de dados pessoais.

3ª Etapa: Monitoramento e Avaliação

Indicadores de desempenho: análise dos principais indicadores.

Gestão de incidentes de segurança de dados.

Análise de resultados: demonstrar a evolução das ações e dos resultados obtidos.

Divulgação dos resultados

Os elementos de governança em privacidade e proteção de dados pessoais não se limitam ao disposto no art. 50 da LGPD. Outros dispositivos legais também abordam o tema de forma relevante, como o art. 46, § 2º, da referida Lei, o qual estabelece que a proteção e a privacidade dos dados devem estar presentes por padrão e desde a fase de concepção de um produto ou um serviço, e durante todo o ciclo de vida dos dados pessoais, em observância aos princípios *Privacy by Design* e *Privacy by Default*.

Ademais, a governança de dados pessoais vai além dos aspectos legais, sendo imprescindível sua integração com as políticas institucionais, a segurança da informação, a implementação de framework de boas práticas de gestão de dados e a gestão estratégica da Instituição. Mais do que implementar programa de governança de dados, o desafio da Instituição é fomentar a cultura de proteção de dados, alinhada com a geração de valor dos serviços baseados em dados.



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

A Resolução CNMP nº 281/2023 reforça esse aspecto ao estabelecer, em seu art. 126, a necessidade de proteção dos dados pessoais desde a concepção e durante todo o ciclo de vida dos projetos, processos, sistemas, bancos de dados, serviços e produtos, atuais e futuros, no âmbito do Ministério Público brasileiro. Os responsáveis devem, nesse contexto, observar princípios específicos relativos à privacidade e proteção dos dados pessoais:

- I – proatividade e prevenção, não reativo nem corretivo;
- II – privacidade como padrão dos sistemas de tecnologia da informação, dos bancos de dados pessoais ou outras práticas de negócio;
- III – privacidade incorporada;
- IV – funcionalidade total;
- V – segurança e proteção, de ponta a ponta, durante o ciclo de vida de tratamento de dados pessoais;
- VI – visibilidade e transparência; e
- VII – respeito pela privacidade do usuário.

A Resolução também estabelece que, da mesma forma, em relação aos softwares e às bases de dados pessoais a serem desenvolvidos ou adquiridos, é imprescindível assegurar que eles incorporem a proteção como requisito desde a sua concepção e por padrão. Isso implica prever, entre outras medidas, atividades de treinamento dos usuários, design, codificação, testes e manutenção adequados.

No que se refere ao treinamento dos usuários, a Resolução estipula que devem ser considerados, no mínimo, os seguintes itens básicos:

I – Internos:

- a) proteção de dados pessoais;
- b) segurança da informação;
- c) controle interno;
- d) gestão de recursos;
- e) análise de riscos; e
- f) requisitos referentes à documentação.

II – Externos:

- a) leis e regulamentações de proteção de dados pessoais;
- b) regulamentações específicas das atividades ministeriais;
- c) importância dos princípios da proteção de dados pessoais; e
- d) direitos dos indivíduos detentores dos dados pessoais.



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

A norma determina que o responsável pelo tratamento deve aplicar, tanto no momento da definição dos meios quanto durante o próprio tratamento, as medidas técnicas e administrativas adequadas. Estas incluem práticas como minimização, pseudonimização e autenticação de dois fatores ou em duas etapas, destinadas a colocar efetivamente em prática os princípios da proteção de dados pessoais e a integrar as garantias necessárias no tratamento.

8. PLANO ESTRATÉGICO

O planejamento estratégico tem por objetivo fornecer soluções de proteção de dados pessoais para cumprir a missão institucional do MPSE.

Para isso, é essencial identificar, de forma concreta e embasada, os reais riscos enfrentados pela Instituição e elaborar um plano de ação. Esse plano deve levar em consideração as prioridades de acordo com a realidade institucional e suas principais necessidades em termos de proteção de dados pessoais. Essas necessidades devem ser traduzidas em medidas e procedimentos divididos nos principais grupos: inventário de dados pessoais, aferição dos riscos associados ao tratamento de dados pessoais, gerenciamento dos riscos e respostas a incidentes de segurança de dados pessoais.

8.1. Inventário de Dados

Para a efetiva proteção de dados pessoais, é crucial identificar o escopo das operações de tratamento de dados, compreendendo quais dados são tratados, como são tratados, por que são tratados, quem é o responsável pelo tratamento e por quanto tempo são armazenados.

Esse diagnóstico pode ser realizado com o auxílio de diversas medidas, como o inventário de dados pessoais e a identificação dos seus fluxos e riscos.

Essas informações podem ser levantadas por meio do mapeamento de dados pessoais, também conhecido como *data mapping*, que é a análise do trajeto que os dados pessoais percorrem desde o momento em que são coletados pela Instituição até o término do seu tratamento. Dessa forma, é possível compreender como os dados pessoais são tratados e como transitam pelo MPSE.

O objetivo desse processo é identificar a origem dos dados, os canais utilizados para coleta, quais dados são tratados, por onde eles fluem, com quem são compartilhados, onde e em quais formatos estão armazenados, para qual finalidade eles são coletados, qual a hipótese legal que justifica o tratamento dos dados e o grau de risco envolvido na coleta de cada informação.



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

Para atingir esse objetivo, o MPSE encontra-se em fase de elaboração de metodologia de identificação dos dados e seus fluxos, utilizando-se de Planilha de Inventário de Dados Pessoais, elaborado pela Secretaria de Governo Digital da União Federal. A planilha deverá ser preenchida por unidades da Instituição, como primeira ferramenta para a coleta das informações. Além de mapear dados, o formulário servirá para identificar e analisar os riscos e para subsidiar a criação de plano de controle setorial e as providências a serem adotadas em cada caso.

8.2. Aferição dos riscos associados ao tratamento de dados pessoais

Uma vez feito o mapeamento e inventário de dados pessoais, o MPSE deverá categorizar os riscos, possibilitando a priorização com base na gravidade, urgência e tendência de cada risco identificado.

8.3. Plano de Gestão de Riscos

O MPSE deverá elaborar um Plano de Gestão de Riscos, eis que a segurança da informação é um dos pontos críticos a serem observados pelas Instituições. Para evitar que algum evento danoso ocorra, é necessário agir preventivamente, identificando as situações que indicam cenários indesejados.

8.4. Plano de Respostas a Incidentes de Segurança de Dados Pessoais

O MPSE deverá adotar um Plano de Comunicação e Resposta a Incidentes de Segurança de Dados Pessoais.

O Incidente de Segurança com Dados Pessoais é conceituado como qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo por meio de acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares dos dados pessoais.

O art. 46 da LGPD estabelece que os agentes de tratamento de dados pessoais devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.



MINISTÉRIO PÚBLICO DO ESTADO DE SERGIPE
PROCURADORIA GERAL DE JUSTIÇA
Expediente nº 20.27.0229.0010790/2024-50

Nesse cenário, o Plano de Resposta a Incidentes de Segurança de Dados Pessoais deve ser estruturado e elaborado para ajudar a identificar, gerenciar e enfrentar incidentes de dados pessoais, com o objetivo de cumprir o disposto nos arts. 48 e 50, inciso I, alínea “g”, da LGPD.

O Plano de Resposta para Incidentes de Segurança de Dados Pessoais do MPSE é instrumento de mitigação dos impactos gerados pelo uso indevido de dados pessoais e de embasamento dos mecanismos de segurança de dados, por meio de instruções e normas procedimentais, conforme o art. 48 da LGPD.

9. CONCLUSÃO

A presente versão inicial do Plano Diretor de Proteção de Dados Pessoais do Ministério Público do Estado de Sergipe busca fixar diretrizes gerais e elencar o conjunto de ações a serem realizadas e temas a serem abordados para solucionar problemas, aprimorar e implementar efetivamente a política de proteção de dados pessoais na Instituição, em consonância com a LGPD e com a Resolução CNMP nº 281/2023.

O plano será monitorado pelo Comitê Estratégico de Proteção de Dados Pessoais do MPSE, assim como atualizado e incrementado no decorrer de sua execução, para se adequar à novas necessidades que venham a surgir, sempre com vistas à tutela do direito fundamental à proteção de dados pessoais, previsto no art. 5º, LXXIX, da Constituição Federal.

Expediente assinado eletronicamente por **Manoel Cabral Machado Neto***, em 27/05/2024 09:48:48, conforme art. 1º, III, "b", da Lei 11.419/2016.



A validade deste documento pode ser conferida no site <https://sistemas.mpse.mp.br/mpse/Administrativo/Publico.html#/Expediente/ConsultaPublica> informando o número do expediente: **20.27.0229.0010790/2024-50**.